Multiple-choice questions for Module 2: IT and Cyber

1. Information security is about protecting information from unauthorized:
a) access
b) use
c) modification
d) all of the above
2. "A process of defining the security controls in order to protect the information assets". This is the definition of:
a) Information management
b) Information security management
c) Information security management protocol
d) Information technology management
3. The C.I.A. triangle includes:
a) Confidentiality
b) Intrusion
c) Confidentiality, intrusion and attacks
d) None of the above
4. Among the necessary tools for information security are:
a) Awareness
b) Training
c) Policy
d) All of the above
5. Among the most necessary tools for information security is:
a) Interconnectedness
b) Education
c) Communication
d) All of the above
6. Among the tools with little to no significance to information security is:
a) Policy
b) Education
c) Awareness
d) None of the above
7. Among the things that can facilitate unauthorized access to a computer by attackers are:
a) Software
b) Hardware
c) Procedural weakness of a safeguard
d) All of the above
8. The absence or weakness of a safeguard that could be exploited is called:
a) Threat
b) Vulnerability
c) Attack
d) Possibility
9. A threat is:
a) The potential danger to information or systems

b) A possibility that someone identifies a vulnerability

c) All of the above

d) None of the above

10. The entity that takes advantage of vulnerability is referred to as:

a) threat agent

b) vulnerability agent

c) risk agent

d) attacking agent

11. "The likelihood of a threat agent taking advantage of vulnerability and the corresponding business impact" is called:

a) Vulnerability

b) Threat

c) Risk

d) Loss

12. In the context of information security, a synonym of risk would be:

a) Threat

b) Hacking

c) Security breach

d) None of the above

13. A cybersecurity safeguard could be:

a) Application

b) Software

c) All of the above

d) None of the above

14. The three types of security control are:

a) Administrative, bureaucratic and technical controls

b) Bureaucratic, policy and physical controls

c) Bureaucratic, logical and physical controls

d) Administrative, technical and physical controls

15. Physical controls, among other things, include:

a) Protecting the perimeter of the facility

b) Controlling individual access into the facility and different departments

c) All of the above

d) None of the above

16. The responsibilities for information security are divided between the following three groups:

a) Senior management, security officers, administrative staff

b) Senior management, functional management, operational management

c) Functional management, security management, administrative staff

d) Functional and operational managers and their staff

17. An information security project team would include:

a) System administrator but not a data custodian

b) Data custodian but not a system administrator or an end user

c) Risk assessment specialists but not security policy developers

d) Data custodian, system administrators, security policy developers